Journal of Autonomy and Security Studies
Vol. 10 Issue 1 (2026)
Research Note

Targeting a Satellite: Electronic Warfare and International Humanitarian Law

Dr. Katariina Simonen

Journal of Autonomy and Security Studies
10(1) 2026, 59–72
DOI: https://doi.org/10.61199/ej90-2p07

Abstract

Satellite signal interference is a core component of electronic warfare. It has become a daily phenomenon in today's conflict zones, considering that most military systems are electric and thereby potential targets of electronic warfare. However, electronic warfare is rather indiscriminate. Its effects are often felt by civilians in third countries, with increasing risks to civil aviation, navigation, telecommunications and humanitarian operations. International humanitarian law sets several requirements for targeting during electronic warfare operations. Yet many legal ambiguities remain, hampering not only the full protection afforded under international humanitarian law but also blurring the threshold of armed conflict. In today's context of erosion of international humanitarian law, there is a pressing need to co-operate on a wide front and inclusively, in order to strengthen and clarify norms on electronic warfare and, thereby, acceptable space behaviors.

Keywords

Electronic warfare, international humanitarian law, targeting, obligation to discriminate

About the Author

Katariina Simonen is Adjunct Professor at the National Defense University (Finland) as well as Visiting Researcher at the Department of World Cultures, University of Helsinki. She is also Pugwash Council Member. Her research interests include law of armed conflict, arms control and legal history.

1. Introduction

The erosion of rules on the use of armed force discussed in the introductory research note to this special issue led to several legal questions in the realm of the law of armed conflict. This follow-up research note intends to discuss more in depth some of those questions when targeting a satellite with the purpose of signal interference or jamming.

There are several Global Navigation Satellite Systems (GNSS) in operation, including China's BeiDou Navigation Satellite System (BDS), Europe's Galileo, Russia's Globalnaja Navigatsionnaja Sputnikovaja Sistema (GLONASS), the USA's Global Positioning System (GPS), India's Regional Navigation Satellite System (IRNSS), and Japan's Quasi-Zenith Satellite System (QZSS). Satellites transmit precise navigation, positioning, and timing information, making them vital for civilian and humanitarian purposes worldwide.

The concept of GNSS interference has been a core component of electronic warfare (EW) for decades. Interference with a GNSS is relatively easy. There are four types of counter-space capabilities: kinetic physical, non-kinetic physical, electronic, and cyber. Kinetic physical operations and capabilities cause permanent and irreversible destruction of a satellite or ground support infrastructure through force of impact by an object or detonation of a warhead. These technologies include direct-ascent anti-satellite (ASAT) missiles and co-orbital systems. ASATs are essentially meant to destroy hostile satellites through the sheer use of high speeds and kinetic energy on impact.[1] Co-orbital systems are satellites placed on similar orbits and can be directed to intercept or interfere with other satellites through close orbital rendezvous operations.

Non-kinetic physical operations involve the use of technology to interfere with or damage space systems without physical contact. Technologies in this category include electromagnetic pulses and directed energy (laser beams or microwave bombardments). A third category is the focus of this note, i.e. electronic warfare (EW) capabilities, using radiofrequency to interfere with or to jam communications to or from satellites but without causing permanent physical damage. The last category is cyber warfare technologies which use software and network techniques to compromise, control, interfere with or destroy computer systems linked to satellite operations. It is important to note that the use of electronic and cyber means have become preferred methods of attack since their use can be plausibly denied. These counter-space capabilities can be used to deny, degrade, disrupt, or destroy space systems. What is more, the requisite technology for electronic and cyber warfare is becoming ubiquitous and diverse, accessible even to non-State actors.[2]

1 Kuplic, Blair Stephenson. 2014. "The Weaponization of Outer Space: Preventing an Extraterrestrial Arms Race." 39 *N.C.J. INT'L L. 1123,* https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=2011&context=ncilj.

2 Rajagopalan, Rajesvari Pillai. 2019. "Electronic and Cyber Warfare in Outer Space*." Space Dossier 3,* UNIDIR https://unidir.org/wp-content/uploads/2023/05/electronic-and-cyber-warfare-in-outer-space-en-784.pdf.

During the Cold War, outer space utilization was primarily for strategic operations, such as strategic intelligence gathering, nuclear attack early warning and executing arms control agreements. Today, space also has a far more important role to play in conventional military operations.[3] What's more, offensive and defensive counter-space operations today would impact not just the security sector but also social and economic sectors across continents because of large-scale civilian dependency on space-based applications. The fact that space is vital to both civilian and military operations increase the danger of inadvertent escalation and conflict if there is, for instance, a disruption or denial of service during a period of heightened tensions. Also, there appears to be a greater willingness to engage in the development and possible use of new offensive counter-space capabilities than those available during the Cold War era. All these developments highlight also the need for clear rules that create the normative context for permissible space behaviors.

2. Defining the context

Electronic attacks are usually done by targeting signals, either through jamming or spoofing. Jamming is a kind of electronic attack that interferes with radiofrequency communications by creating noise in the same frequency band and within the field of view of the antenna of the satellite or receiver it is targeting, thus disrupting communications. Jamming causes temporary disturbance and disruption and is thus reversible. Once the jammer is turned off, the communication can return to normal. Spoofing is another form of electronic attack where a fake signal is produced by the attacker's device. In this case, if the spoofing attack targets the downlink data from a satellite to the ground, it could end up feeding false or corrupt data into the ground receiver system. Hijacking a satellite command and control and feeding it with such data are well-known means of disruption.[4] Satellites are controlled from ground stations through electronic signals, and they pass their data back to ground stations, so attacking those uplink and downlink linkages electronically can render satellites ineffective.[5]

With a satellite's signal interference, we enter the realm of EW, which involves the exploitation of the electromagnetic spectrum (EMS) to disrupt, disable or destroy an adversary's ability to use the EMS. The EMS spans a wide range of wavelengths which provides maneuver space consisting of all frequencies of electromagnetic radiation,

3 *Ibid*. 3.

4 Poirier, Clémence. 2025. "Electronic and Cyber Operations Against Space Systems". *Policy Perspectives* Vol. 13/1, https://css.ethz.ch/en/center/CSS-news/2025/01/electronic-and-cyber-operations-against-space-systems.html.

5 Harrison, Todd, Johnson, Kaitlyn and Roberts, Thomas G. 2019. *Space Threat Assessment 2019.* Center for International and Strategic Studies, https://aerospace.csis.org/wp-content/uploads/2019/04/SpaceThreatAssessment2019-compressed.pdf.

including radio waves, microwaves, infrared radiation, visible light, ultraviolet radiation, x-rays and gamma rays.[6] For instance, military operators use a host of equipment including receivers, transmitters, and satellites to communicate within the EMS operating environment, thus enabling the "command and control" warfighting function in military operations.[7] In fact, EW is no new phenomenon on the battlefield. To the contrary, different types of activities in the electromagnetic spectrum have been an integral part of warfare and other military activities since the early part of the 20th century – first as a means of intercepting enemy communication, later also in the shape of offensive and defensive interference with different types of weapons, communication and positioning systems, often in support of kinetic operations.[8]

Technological development has led to a situation where most military systems on the battlefield are electric and thereby potential targets of electronic warfare. The ongoing conflict in Ukraine serves as an illustration of the prominent – albeit in many cases invisible – role of EW. Both sides of the conflict have used EW for various purposes including targeted information campaigns against enemy soldiers and spoofing and jamming of enemy weapons systems.[9] Given the key role communications equipment and sensors play in military operations, it is unsurprising that electronic warfare is an important aspect of joint military operations for purposes of interference with an adversary's sensing, communication, and navigation capabilities.[10]

The ITU (International Telecommunications Union) Radiocommunication Bureau has noted rising electromagnetic interference since 2019 and previously warned about risks to global navigation services in 2022.[11] Russian EW operations such as jamming and spoofing have been interfering with non-military activities in northern Norway and in Finland even before ITU's recent reports. For instance, in 2017 Russia's EW interfered with NATO exercises in the region (Trident Juncture).[12] In this case, the EW signal emitted by Russia also served as 'signaling' to NATO its discontent with the large-scale exercise taking place near the Kola Peninsula – home to Russia's Northern Fleet and other strategic units.[13] Nowadays, such electromagnetic interference has also become a daily occurrence

6 Lawless, Robert and Nasu, Hitoshi. 2024. "Electronic warfare and the law of armed conflict". *Articles of War.* Lieber Institute, West Point, https://lieber.westpoint.edu/electronic-warfare-law-armed-conflict-2/.
7 *Ibid.*
8 Graff, Ulrik and Iben, Yde. 2023. "Elektronisk krigsførelse i folkeretligt perspektiv". University of Copenhagen, iCourts, https://jura.ku.dk/icourts/research/intermil/legal-aspects-of-electronic-warfare/.
9 *Ibid.*
10 Lawless and Nasu, footnote 6.
11 Poirier, footnote 4.
12 Harvey, James. 2025. "The Russo-Ukrainian war's expansion into the High North poses electronic warfare challenges for NATO". *The Barents Observer,* https://www.thebarentsobserver.com/opinion/the-russoukrainian-wars-expansion-into-the-high-north-poses-electronic-warfare-challenges-for-nato/431197.
13 *Ibid.*

in northeastern Europe. From the airport of Gdansk through the busy shipping lanes of the Baltic Sea and all the way to the airspace of Estonia and Finland, these interferences have been recorded almost daily since Russia's full-scale invasion of Ukraine in February 2022.[14] Recently, civilian aviation, satellite navigation and other GPS users in Norway's East Finnmark region have been particularly affected by Russian EW activities.[15] Russia's increased EW activity in the region since late 2024 seems to be a response to Ukrainian long-range drone attacks on the strategic weaponry Russia has based in the Kola peninsula.[16]

In terms of international humanitarian law (IHL), military objectives of the opponent (like the Ukrainian drones) are legitimate targets in armed conflict. However, non-belligerents also suffer from Russian EW activities. From the point of view of third states affected, Höller's short article questioning the official narrative of regional states regarding Russia's EW operations as hybrid warfare is interesting.[17] According to Höller, the official narrative regarding Russia's EW operations in the Baltic might not count as hybrid warfare, due to lack of intention to harm. Accordingly, the interference over the Baltic Sea and in neighboring NATO states could be largely collateral, and not the point of the operation itself.[18] Considering that the obligation of distinction between military and civilians is a core rule of IHL, Russian EW operations pose interesting challenges from the point of view of targeting, attack, and its intended or foreseeable consequences, which shall all be discussed below.

3. International humanitarian law and targeting

3.1 Applicable rules

As with all military operations, the use of EW capabilities during armed conflict must comply with the law of armed conflict (*jus in bello*). As the law of armed conflict is framed in terms of people and objects, any analysis of legal requirements regarding military operations in the EMS sphere must appreciate the extent to which such operations impact people and objects.[19]

14 Höller, Linus. 2025. "Researchers home in on origins of Russia's Baltic GPS jamming". *Defense News Europe,* https://www.defensenews.com/global/europe/2025/07/02/researchers-home-in-on-origins-of-russias-baltic-gps-jamming/.
15 Harvey, footnote 14.
16 Staalesen, Atle. 2024. "Governor: Murmansk is under drone attack". The Barents Observer, https://www.thebarentsobserver.com/news/governor-murmansk-is-under-drone-attack/102409; Nilsen, Thomas. 2025. "Successful and devastating: Massive drone attacks on Olenya airbase". *The Barents Observer*, Successful and devastating: https://www.thebarentsobserver.com/security/successful-and-devastating-massiv-drone-attacks-on-olenya-airbasenbsp/430777Massiv drone attacks on Olenya airbase.
17 Höller, footnote 14.
18 *Ibid*.
19 Lawless and Nasu, footnote 6.

The key norms for our purposes are codified in Parts III and IV of the Additional Protocol I to the Geneva Conventions.[20] Parts III and several chapters of Part IV (Arts. 35–60) deal with the conduct of hostilities, i.e. questions which hitherto were regulated by the Hague Conventions of 1899 and 1907 and by customary international law. Their reaffirmation and development were important considering the age of the Hague conventions. Among the most important Articles are those on the protection of the civilian population against the effects of hostilities. They contain a definition of military objectives and prohibitions of attack on civilian persons and objects.

The very core norm regarding means and methods of warfare (Part III) is article 35, which stipulates as a basic rule that the right of the Parties to the conflict to choose methods or means of warfare is not unlimited. Prohibited means and methods are those which are of a nature to cause superfluous injury or unnecessary suffering, or which are intended, or may be expected, to cause widespread, long-term, and severe damage to the natural environment. As far as new weapons (their study, development, acquisition, or adoption) are concerned, Article 36 obliges the High Contracting Parties to determine whether their employment would, in some or all circumstances, be prohibited by AP I or by any other rule of international law applicable to the High Contracting Party.

In turn, the very basic rule for the protection of civilians and their distinction is confirmed by Article 48. It is the very foundation on which the codification of the laws and customs of war rests[21]: the civilian population and civilian objects must be respected and protected in armed conflict and for this they must be distinguished from combatants and military objectives.[22] This obligation of distinction applies at all times and it is noteworthy that it concerns all civilians, also civilians of the non-belligerents, like civilians of states affected in the Baltic and High North regions.

Article 49 defines 'attacks' as acts of violence against an adversary, whether in offence or defense. Civilian population is defined in Art. 50 by exclusion of members of armed forces as defined in Article 43 and Article 4 A (1)–(3) and (6) of the Third Geneva Convention. In case of doubt whether a person is civilian, that person shall be considered to be a civilian.

Article 51 specifies that the civilian population, as well as individual civilians, shall not be the object of an attack; also, acts or threats of violence with the primary purpose of spreading terror among the civilian population are prohibited. The said article further

20 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, International Humanitarian Law Databases, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977.

21 Sandoz, Yves and Swinarski, Christophe and Zimmermann, Bruno (eds.). 1986. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, International Committee of the Red Cross, 1875.

22 Commentary of 1978 – Article 48 Basic Rule, International Humanitarian Law Databases, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-48/commentary/1987?activeTab=.

prohibits indiscriminate attacks. Points a–c are relevant from the point of view of evaluating the legality of EW operations:

a) those which are not directed at a specific military objective;
b) those which employ a method or means of combat which cannot be directed at a specific military objective; or
c) those which employ a method or means of combat the effects of which cannot be limited as required by this Additional Protocol I; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

The Article provides further examples of types of attacks that are to be considered as indiscriminate due to lack of proportionality vis-à-vis the military advantage anticipated. According to point 5.b of Article 51 (which is again relevant for EW and third states), an attack that is considered indiscriminate is:

b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

Article 52 (General protection of civilian objects) further dictates that attacks shall be limited to strictly military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

Article 57 includes an obligation of constant care in the conduct of military operations to spare the civilian population, civilians, and civilian objects as well as a set of precise obligations of precaution (including *incidental* loss of life and evaluation of proportionality vis-à-vis military necessity):

a) for those who plan or decide upon an attack to do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives;
b) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects;
c) refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

Also, the Article requires that an attack shall be cancelled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated. In point 4 of the said Article, it is required that in the conduct of military operations at sea or in the air (relevant, again, for EW operations), each Party to the conflict shall, in conformity with its rights and duties under the rules of international law applicable in armed conflict, take all reasonable precautions to avoid losses of civilian lives and damage to civilian objects.

Hence, AP I sets several requirements for distinction between civilian and military, a prohibition of specific means of warfare as well as principles of proportionality and precaution for those planning and conducting attacks.

3.2 Testing the limits of Additional Protocol I – Attacks

The intriguing challenge is the application of AP I rules just described above to the realm of EW. The legal evaluation of EW under AP I is related to the concept of attack and its threshold, whereas operations below such a threshold are more problematic. It is also important to note at this point that the concept of attack for purposes of targeting is different from the concept of attack under the law of self-defense in UN Charter Article 51 and customary law.

Now, when considering the law of targeting under humanitarian law, weapon systems that cause physical harm, injury or death usually raise no critical legal questions about the attack threshold. Hence, the attack threshold is defined by its consequences, rather than by means or intent.[23] Indeed, the EMS may be used to inflict concrete damage in this sense, by means designed to cause physical destruction such as directed energy weapons like high-energy lasers and high-power microwaves.[24] Many jurists would agree that the use of EMS can be deemed an attack when it is reasonably expected to cause an injurious or damaging effect.[25]

The attack assessment becomes more difficult when an EW capability is designed to cause temporary, non-kinetic effects while creating a risk of potential physical damage. According to Graff and Iben, most EW means "only" temporarily jam the system targeted by the attack or cause it to function in an unintended manner for a certain time, so that

23 Graff and Iben, footnote 8.
24 Office of Naval Research. "Directed Energy Weapons: High Power Microwaves", https://www.onr.navy.mil/organization/departments/code-35/division-353/directed-energy-weapons-high-power-microwaves.
25 Lawless and Nasu, footnote 6.

most actions carried out in the EMS are not considered attacks.[26] However, when EW operations cause physical consequences (death, injury or destruction), the attack threshold may be crossed. For instance, this might be the case if jamming causes the collision of an aircraft or spoofing causes a ship to run aground. In such cases, EW operations need to comply with basic rules of the AP I regarding distinction, proportionality, and precaution. The said applies to operations that are intended or can be reasonably expected (foreseeable result) to cause destruction. The opponent's military targets (AP I Art. 52.2) are *per se* legitimate targets for an adversary's attack operations.

When discussing the effects of EW operations on civilians and civilian objects, AP I articles of distinction (Art 48), proportionality and prohibition of indiscriminate attacks (Art. 51), legitimate military targets (Art. 52.2) and principle of precaution (Art. 57) find full application. The principle of distinction under Art. 48 includes all civilians, also those of non-belligerents. Hence, the effects of signal jamming and interference in conflict zones by High Contracting Parties' military planners need to incorporate the evaluation of EW operations' foreseeable effects to all civilians, include a proportionality check of effects of military operations versus gained military advantage, and take all precautionary measures to protect the civilians and civilian objects. The attack must be directed at legitimate military targets and the incidental harm it is expected to inflict upon civilians and civilian objects must not be out of proportion to the anticipated military advantage.[27]

So far there is relatively little professional analysis of EW operations and requirements stemming from international humanitarian law, but the rules on cyber warfare in *Tallinn Manual 2.0* (which, by the way, also uses the EMS) as well as discussions regarding electromagnetic microwave counter-IED (improvised explosive devices) weapons in Additional Protocol II environments (i.e. in cases of non-international armed conflicts) provide for useful analogies, especially when analyzing whether the military capability is employed in conformity with the targeting rules, including precautions in case of an attack.[28] Also, in the commentary to Art. 36 of the AP I (New Weapons), experts raised concerns regarding the indiscriminate character of EW (amongst others), as follows:

> "Quite independently of the problems of atomic (nuclear), bacteriological and chemical warfare, or space war, which have not been included in this context, the experts were concerned with geophysical, ecological, electronic and radiological warfare as well as with devices generating radiation, microwaves, infrasonic waves, light flashes and laser beams. The use of long-distance, remote-control weapons, or weapons connected to sensors positioned in the

26 Graff and Iben, footnote 8.
27 Lawless and Nasu, footnote 6.
28 Schmitt, Michael N. (ed.). 2017. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press N.Y., p. 373–562; Boothby, William. 2016. *Weapons and the Law of Armed Conflict (2nd ed.).* Oxford University Press, p. 346–365.

> field, leads to the automation of the battlefield in which the soldier plays an increasingly less important role. The countermeasures developed as a result of this evolution, *in particular electronic jamming (or interference), exacerbates the indiscriminate character of combat.* In short, all predictions agree that if man does not master technology, but allows it to master him, he will be destroyed by technology."[29]

The question remains, then, whether EW operations can be executed in a discriminate manner or not. If not, the contradiction with the very basic rule of discrimination becomes evident.

3.3 Special challenges arising from EW

One challenge arises from military operations using EW below the attack threshold. As already mentioned above, most EW operations "only" temporarily jam the target system or cause its unintended function for a certain time. Due to their non-violent and often temporary effect, such EW operations cannot be considered attacks. International law on operations below the attack threshold is less clear.[30] However, Art. 48 basic rule on the protection of civilians has wider applications in that its applicability extends beyond attacks. The Article speaks of "military operations" which must be directed only against military objectives. With regard to EW, this means that many activities fall within the scope of Art. 48 even if they cannot be considered attacks.[31]A further challenge arises from the fact that military operations are not defined in AP I (or AP II or the Geneva Conventions). However, contextual reading of the entire Section IV on the protection of the civilian population refers to military operations in which violence is used, and not ideological, political or religious campaigns.[32]

Some military operations may not include violence, though, for instance attempts to influence the opponent and/or civilians. In such cases other rules of international humanitarian law may apply, such as the prohibition to threaten the adversary that there shall be no survivors (Art. 40 of AP I).[33] Other EW operations are more difficult to evaluate, especially if these are EW operations in support of military operations without being directly linked to such military operations. As examples, Graff and Iben cite interfering with civilian communications in order to prevent civilians to give warning of

29 Commentary of 1978 – Article 36 New Weapons, International Humanitarian Law Databases, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36/commentary/1987?activeTab=1949GCs-APs-and-commentaries, 1476.
30 Graff and Iben, footnote 8.
31 *Ibid.*
32 Sandoz et al., footnote 21, 1875.
33 Graff and Iben, footnote 8,

troop movements in a specific region or the establishment of so-called ECM (electronic countermeasure) bubbles around military objectives; the principle of distinction may apply depending on the circumstances, the former example being the more problematic one as these are acts that target civilians directly.[34]

Another issue concerns the prohibition of perfidy under Art. 37 of AP II. Acts that invite the confidence of an adversary, leading him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law of armed conflict, with the intent to betray that confidence. Such acts may involve, for instance, the feigning of an intent to negotiate under a flag of truce or of a surrender, the feigning of an incapacitation by wounds or sickness, the feigning of civilian, non-combatant status or the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other States not parties to the conflict.[35] However, ruses of war are permitted. Article 37.2 of AP I specifies that ruses are acts which are intended to mislead an adversary or to induce him to act recklessly, but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law.[36] Examples given by the article include the use of camouflage, decoys, mock operations and misinformation.

In case of EW operations, it is obvious that they need to respect the prohibition of perfidy under Article 37.1 of AP I. At the moment, there is an ongoing discourse in naval warfare that includes aspects that may be relevant for EW. The question is whether the right to sail under false flag may be interpreted to cover the sending of false radar and acoustic signals.[37]

A third issue concerns special protection afforded under international humanitarian law, such as medical establishments, units, and personnel.[38] The importance of their protection during both international as well as non-international armed conflict is evidenced by extensive protection rules both in the Geneva Conventions II as well as AP I–II.[39] Relevant for our discourse is the fact that belligerent parties are not only prohibited from making hospitals and mobile medical units objects of an attack but also from interfering with their work. Hence, the question is whether the use of EW, for instance, to disrupt communications can be construed as interfering with medical services or unnecessarily preventing their

34 *Ibid.*
35 Additional Protocol I, Article 37.1.
36 *Ibid*., Article 37.2.
37 Graff and Iben, footnote 8, with reference to *Militærmanual om folkeret for danske væbnede styrker i internationale militære operationer* 2020, https://www.forsvaret.dk/da/publikationer/militarmanual/, p. 580–581.
38 Civil defense organizations are also awarded special protection under AP I Articles 61–66.
39 See for instance Geneva Convention I, Ch. III, Arts. 19–23 regarding medical units and establishments; Ch. IV, Arts. 24–32 regarding personnel; Ch. V, Arts. Arts. 33–34 on buildings and material; Ch. VI, Arts. 35–37 regarding medical transports and Ch. VII, Arts. 38–44 regarding the distinctive emblem.

proper functions, even if an attack threshold is not crossed? According to Lawless and Nasu, communications used for medical services are technically indistinguishable from other communications taking place in the conflict zones, as hospitals do not emit a special kind of electromagnetic wave and they do not necessarily transmit on a special frequency which would allow military operations immediately to identify them as hospitals.[40]

Regardless, a recent commentary regarding Art. 19 of the 1st Geneva Convention on protection of medical units and establishments extends the obligation to respect and protect military medical establishments and units to the prohibition of an intentional disruption of these units' ability to communicate for medical purposes with other components of the armed forces.[41]

The risks of harmful interference for humanitarian assistance vehicles were also underlined in a recent joint statement issued by three UN agencies, the ITU, the ICAO (International Civil Aviation Organization) and the IMO (International Maritime Organization), as follows:

> "NOTING with grave concern the increasing number of cases of harmful interference in the form of jamming and spoofing affecting the Radio Navigation Satellite Service (RNSS), which is critical for navigation of civil aircraft, maritime vessels, humanitarian assistance vehicles, as well as for time synchronization of telecommunication networks…
>
> ITU, ICAO and IMO jointly and urgently call on their respective Member States to protect the RNSS from transmissions that can adversely cause harmful interference degrading, interrupting or misleading signals used for civilian and humanitarian purposes."[42]

As noted above in the previous section, EW is bound to exacerbate the indiscriminate character of conflict. Hence, the challenge lies in the distinction of civilians from the military in the EMS in general, and the identification of hospitals based on EMS activity in particular.

40 Lawless and Nasu, footnote 6.

41 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949, Commentary of 2016, Article 19, https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-19/commentary/2016?activeTab=#_Toc452045289,1804.

42 Joint Statement by the Secretary General of the International Telecommunication Union, the Secretary General of the International Civil Aviation Organization, the Secretary General of the International Maritime Organization regarding PROTECTION OF THE RADIO NAVIGATION SATELLITE SERVICE FROM HARMFUL INTERFERENCE, 25 March 2025, https://www.itu.int/en/mediacentre/Pages/PR-2025-03-25-radio-navigation-satellite-service-harmful-interference.aspx.

4. Concluding remarks

The EW environment is quite challenging for military planners. Regardless, efforts need to be made to create a better understanding of the requirements for EW planning stemming from IHL. Making sure that key concepts of distinction, proportionality and precaution as well as special protections afforded under IHL (medical units, personnel, equipment *et cetera*) are part of the military planning is the responsibility of every High Contracting Party.

The realm of EW is under-researched terrain in terms of international law. As evidenced by the discussion above, topics for further research are many: the concept of attack in all cases of EW (also when physical consequences are not easily foreseeable), EW operations under the threshold of attack and the applicable legal framework, the concept of military operations, the principle of distinction and third states and so forth.

The threshold of (armed) EW attack from the point of view of self-defense, especially by third states, also needs clarification, considering that armed forces of states may relatively easily find themselves in opposition in the realm of EW. One needs only to think of NATO's developing EW capabilities and their potential use against Russian EW interference. The threshold of armed conflict becomes an interesting question for legal advisors in such a quite foreseeable situation. Prudence would seem to dictate that interpretative questions are to be solved sooner rather than later.

These interpretative challenges occur in a time and context which is very challenging from the point of view of IHL's continued respect by states. International Committee of the Red Cross (ICRC) published last December its *Humanitarian Outlook 2026: A World Succumbing to War* -report with alarming humanitarian tendencies.[43] One of these is the erosion of IHL evidenced by on-going conflicts and complete disregard for IHL by states and non-state actors. This situation does not change the conclusion regarding the importance of working to clarify the legal interpretation of IHL for EW operations, but rather strengthens it and underlines the need for enhanced co-operation in diverse formats. For instance, ITU, mandated to act on electronic operations against satellites, could join forces with the ICRC and provide the technical advice needed for clarifying different facets of EW operations under IHL.[44] Also, States that are known defenders of human rights and humanitarian law (Switzerland, Ireland, Norway, Austria, Mexico *et cetera*), NGOs, and academia have joined forces before to accomplish significant humanitarian conventions like the Mine Ban Treaty (1999), the Convention on Cluster Munitions (1999) and the Treaty Prohibiting Nuclear Weapons (2021). A similar effort for the defense of

43 ICRC. 2025. *Humanitarian Outlook 2026: A world succumbing to war,* https://www.icrc.org/en/article/humanitarian-outlook-2026.

44 Poirier, footnote 4.

international humanitarian law and for strengthening its application in fields like EW would be a welcome initiative.

On a grassroots level, the use of military capabilities depends on military advisors. Several states have published military manuals for their armed forces, but most states have not (like Finland, Sweden, or Russia). There are also overarching military manuals for specific environments like the *Tallinn Manual 2.0* for cyber operations[45] and the *Woomera Manual* of military space operations[46], which have been prepared by experts in consultations with States. Similar initiatives could be one possibility to harness the legal expertise of different states to forge an understanding of the application of IHL in diverse EW operations. If inclusive, meaning the inclusion of experts of all willing states, such exercises could have significant power to affect the applicability of rules of IHL to EW operations.

Finally, we shall be heading back to space. Fundamentally, the question is of acceptable space behaviors. Targeting a satellite with civilian functions should be deemed highly condemnable, and space-faring nations should aim to forge a consensus on this point. Dual-use satellites are evidently more problematic, but the respect for IHL should be enhanced in such cases. Hence the importance of inclusion of IHL in relevant discussions in Geneva and Vienna. Purely military satellites are another matter, as these are a military target *per se*. However, they are not a military target if they are operated by a non-belligerent. Hence, the pursuit of a consensus on acceptable space behaviors, better understanding of IHL requirements, along with technological developments to allow for better protection and attribution in cases of illegal targeting, are concrete steps necessary for a rule-based order in international relations.

45 Schmitt, footnote 28.

46 Beard, Jack and Stephens, Dale (eds.). 2024. *The Woomera Manual on the International Law of Military Space Operations*. Oxford University Press, https://doi.org/10.1093/law/9780192870667.001.0001.